Attorney's Docket No.: 13838-002001 / FGN/43011

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant : Eric Coates et al.
Serial No. : 10/052,896
Filed : January 15, 2002
Title : CONSENSUS PROTECTED DATABASE

Art Unit : 2171
Examiner : Unknown

Commissioner for Patents
Washington, D.C. 20231

TRANSMITTAL OF PRIORITY DOCUMENT UNDER 35 USC §119

Applicant hereby confirms his claim of priority under 35 USC §119 from the following application(s):

·United Kingdom Application No. GB 0101131.1 filed January 16, 2001

·United Kingdom Application No. GB 0109281.6 filed April 12, 2001

A certified copy of each application from which priority is claimed is submitted herewith.

Please apply any charges or credits to Deposit Account No. 06-1050.

Respectfully submitted,

36,518
Diane Gardner for
Scott C. Harris
Reg. No. 32,030

Date: May 15, 2002

Fish & Richardson P.C.
4350 La Jolla Village Drive, Suite 500
San Diego, California 92122
Telephone: (858) 678-5070
Facsimile: (858) 678-5099

10183328.doc

CERTIFICATE OF MAILING BY FIRST CLASS MAIL

I hereby certify under 37 CFR §1.8(a) that this correspondence is being deposited with the United States Postal Service as first class mail with sufficient postage on the date indicated below and is addressed to the Commissioner for Patents, Washington, D.C. 20231.

May 15, 2002
Date of Deposit

Gina Bianchi
Signature

Gina Bianchi
Typed or Printed Name of Person Signing Certificate

The Patent Office
Concept House
Cardiff Road
Newport
South Wales
NP10 8QQ

I, the undersigned, being an officer duly authorised in accordance with Section 74(1) and (4) of the Deregulation & Contracting Out Act 1994, to sign and issue certificates on behalf of the Comptroller-General, hereby certify that annexed hereto is a true copy of the documents as originally filed in connection with the patent application identified therein.

I also certify that the attached copy of the request for grant of a Patent (Form 1/77) bears an amendment, effected by this office, following a request by the applicant and agreed to by the Comptroller-General.

In accordance with the Patents (Companies Re-registration) Rules 1982, if a company named in this certificate and any accompanying documents has re-registered under the Companies Act 1980 with the same name as that with which it was registered immediately before re-registration save for the substitution as, or inclusion as, the last part of the name of the words "public limited company" or their equivalents in Welsh, references to the name of the company in this certificate and any accompanying documents shall be treated as references to the name with which it is so re-registered.

In accordance with the rules, the words "public limited company" may be replaced by p.l.c., plc, P.L.C. or PLC.

Re-registration under the Companies Act does not constitute a new legal entity but merely subjects the company to certain additional company law rules.

Signed

Dated 17 APR 2002

Patents Form 1/77
Patents Act 1977
(Rule 16)

The Patent Office

17JAN01 E598440-2 D02917
P01/7700 0.00-0101131.1

Request for grant of a patent

The Patent Office
Cardiff Road
Newport
South Wales NP10 8QQ

1. Your reference
5374601/JP

2. Patent Application Number **0101131.1** 16 JAN 2001

3. Full name, address and postcode of the or of each applicant *(underline all surnames)*

Abattia Group Ltd.
88 Onslow Gardens
London
SW7 3BS

Patents ADP number *(if known)* 8062606001

If the applicant is a corporate body, give the country/state of its incorporation Country: England

4. Title of the invention

DATA PROTECTED DATABASE

5. Name of agent ~~Beresford & Co~~ REDDIE + GROSE

"Address for Service" in the United Kingdom to which all correspondence should be sent ~~2/5 Warwick Court High Holborn London WC1R 5DH~~ 16 THEOBALDS ROAD LONDON WC1X 8PL

Patents ADP number 1826001

6. Priority details

Country	Priority application number	Date of filing

Patents Form 1/77

7. If this application is divided or otherwise derived from an earlier UK application give details

Number of earlier application | Date of filing

8. Is a statement of inventorship and or right to grant of a patent required in support of this request?

YES

9. Enter the number of sheets for any of the following items you are filing with this form.

Continuation sheets of this form	-
Description	49
Claim(s)	-
Abstract	-
Drawing(s)	-

10. If you are also filing any of the following, state how many against each item.

Priority documents	-
Translations of priority documents	-
Statement of inventorship and right to grant of a patent *(Patents form 7/77)*	-
Request for preliminary examination and search *(Patents Form 9/77)*	-
Request for Substantive Examination *(Patents Form 10/77)*	-
Any other documents *(please specify)*	-

11. I/We request the grant of a patent on the basis of this application

Signature _____ Date 16 January 2001
BERESFORD & Co

12. Name and daytime telephone number of person to contact in the United Kingdom

DR. JANET FRANCES PERKINS

Tel: 020 7831 2290

DATA PROTECTED DATABASE

1. OBJECTIVES

The objective of the Generic System for Consensual Processing of Personal Data ("Generic SCPPD") is to provide a tool for any entity ("Data Controller") needing – or wishing – to obtain, hold, display or process (all the foregoing together hereinafter referred to as "Processing") personal data regarding an individual ("Data Subject") within a framework in which the Data Subject's consent for such Processing is sought. Specific examples of occasions in which this might occur include, without limitation, situations where a Data Controller operates within the confines of EU Data Protection Directives or any similar regulatory or voluntary codes in these or any other jurisdictions worldwide.

Essentially, the Generic SCPPD allows the Data Controller to have its database of Data Subjects' personal data (consisting of one or more Personal Data Items per Data Subject, where such a Personal Data Item could be any qualitative or quantitative personal data relating to the Data Subject, which might include, without limitation, name details, contact details, family details, health details, financial details, lifestyle details, life stage details, life events details, demographic details, any details relating to the Data Subject's relationship to the Data Controller, any qualitative comment relating to the Data Subject, or any other such personal data, including photographs) secure, accessible and updateable over the Internet.

2. BUSINESS DESIGN

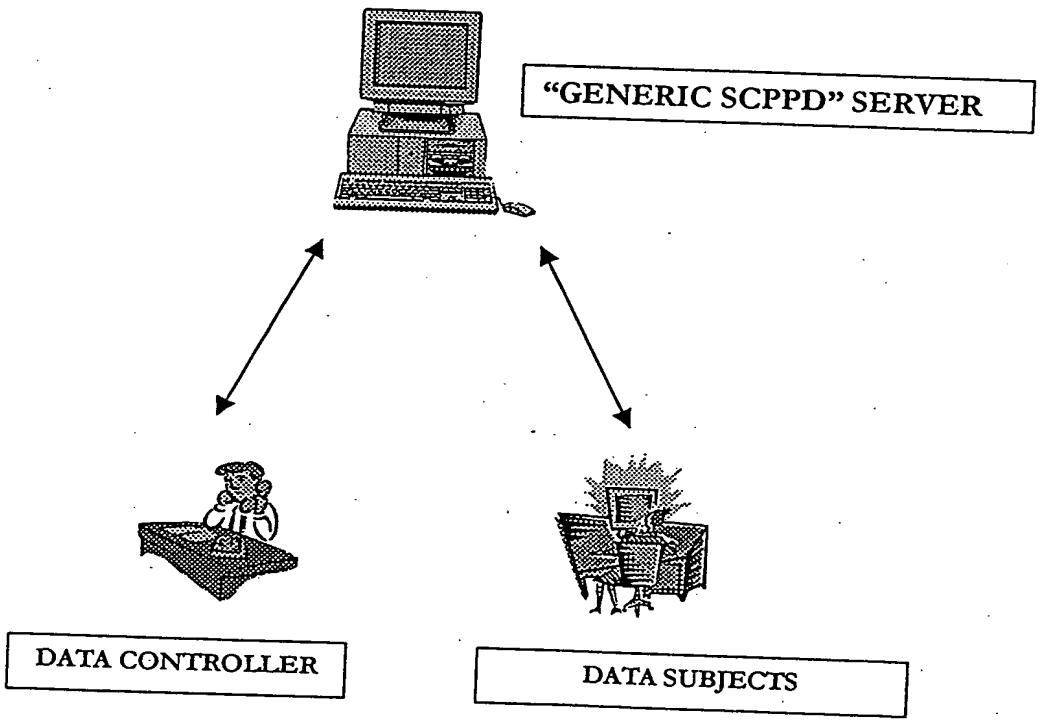
2.1 OVERVIEW

2.1.1 Users

The Generic SCPPD has two classes of user, the Data Controller, and the Data Subjects. The Data Controller will be able to see and change all Personal Data Items held on the database regardless of the Data Subject to which they refer and will be able to Process the Personal Data Items. The Data Subjects will be able to see their own Personal Data Items. The user group is a "closed" user group, and access is password protected and limited. Data Subjects may, or may not, be located in the same country as the Data Controller, and the Data Controller may need – or wish – to Process the Personal Data Item differently depending on the country of location of the Data Subject.

2.1.2 Logical System Architecture

The Generic SCPPD will be hosted on a server and will be accessible through the Internet by the Data Controller and the Data Subjects based on the permissions granted by the Data Controller.



2.1.3 Screen Design

For the Data Controller all data entry screens can be used in search mode; enabling the Data Controller to search for one or more Data Subjects on the basis of a Data Subject's name. For example, the Data Controller can enter a Data Subject's name, or a wildcard (denoted by a partial name followed by an asterix), and the system will display the first occurrence of the name or the names that meet the wildcard criterion and allow the Data Controller to scroll through to the Data Subject required.

2.1.4 Data Fields

Each Data Item will be classified as belonging to a Default Processing Group, which specifies how such a Data Item is to be Processed prior to explicit consent for processing being obtained from the Data Subject, i.e. the period between the data "going live" on the database following entry by the Data Controller and the first time it is verified by the Data Subject. This classification allows the Data Controller to account for different processing requirements or restrictions that might apply to particular types of data, such as the differing treatments of so-called "sensitive" and "non-sensitive" data under the UK's 1998 Data Protection Act.

Personal Data Items are those Data Items that relate to a specific Data Subject. Each Personal Data Item should be stamped with four elements of information:

- The date that the integrity of the Personal Data Item was last verified by the Data Subject. (See 2.1.6, Integrity of Personal Data Item). This integrity is determined either by being viewed online, or via response to a report sent by the Data Controller to the Data Subject, which is corrected and returned to the Data Controller. This field is called Date-Last-Correct.
- The User ID of the last person to update the Personal Data Item. This field is called Last-Changed-By.
- The date the Personal Data Item was last updated. This field is called Last-Changed-On.
- Whether the Data Subject has consented to the Personal Data Item being subjected to the Specified Processing described by the Data Controller (see 2.1.5, Consent for Specified Processing).

2.1.5 Consent for Specified Processing

The Data Controller will explicitly specify to the Data Subject all Processing that is to be performed on the Data Items, and also that Data Items are to be viewable over the Internet by the Data Controller and by the Data Subject. The Data Controller will seek to obtain the Data Subject's consent for such Processing as a condition for the Data Subject using the system. Prior to the first time that the Data Subject's consent is obtained for Specified Processing, the Default Processing associated with the Default Processing Group to which the Data Item belongs will govern processing.

2.1.6 Integrity of Personal Data Item

If, having viewed a Personal Data Item, a Data Subject does not seek to change the Personal Data Item data, it is assumed that the Data Subject has confirmed the integrity of the Personal Data Item. For each Personal Data Item on the system, the Generic SCPPD will record the date and the time last changed or verified by the Data Subject, together with the identity of the Data Subject changing the Personal Data Item. The Data Controller can confirm the data integrity or change or remove Personal Data Items with the consent from the Data Subject.

2.1.7 Database Searching

If a Data Subject requests that the Data Controller report what Personal Data Items relating to that Data Subject are held on the database, the Data Controller will be able to search the database for the Personal Data Items relating to the Data Subject and provide the Data Subject with a paper or e-mail report of the Personal Data Items.

2.1.8 Proactive Consent

The Data Controller will be able to seek consent for the Processing of Personal Data Items, and confirmation of the integrity of Personal Data Items, from each Data Subject who is unable or chooses not to access the Generic SCPPD via the Internet. Printing and sending a report to the Data Subject for confirmation will achieve this.

2.1.9 Security

The system will be protected against unauthorised access. The Data Controller will issue each Data Subject with a username and password with which to gain authorised access to the system.

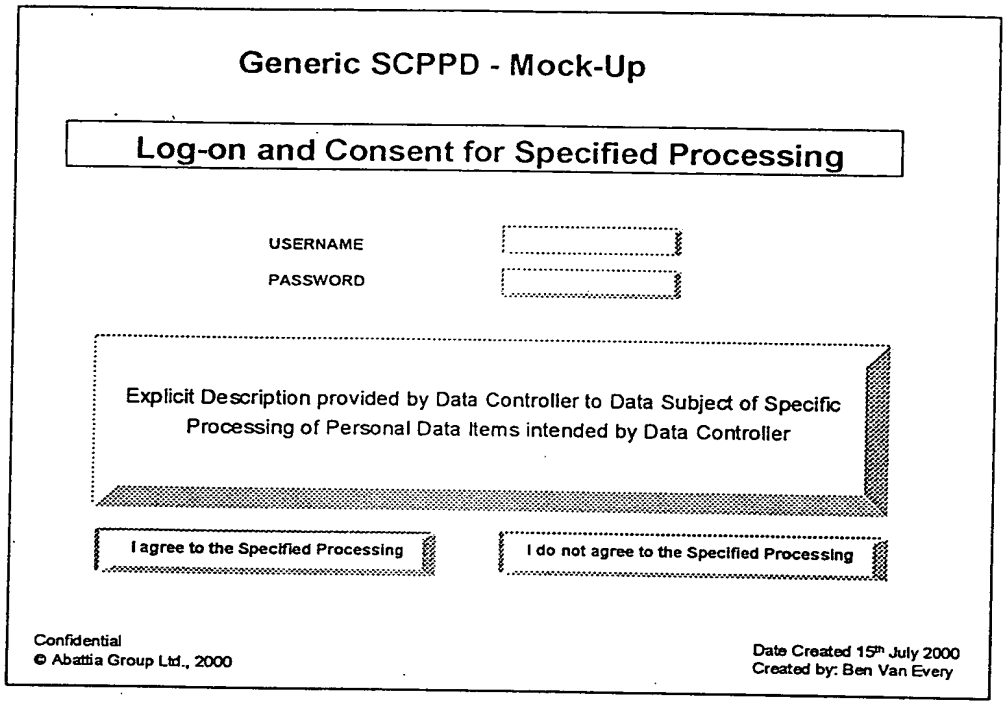
2.1.10 Displaying Information

All information is available to the Data Controller. The Data Subject can see his or her own Personal Data Items, either through the Internet, or from a printed/ e-mailed report supplied by the Data Controller.

2.1.11 "Processing" of Personal Data Items

As the Generic SCPPD is intended as a "generic" engine, no description is given herein of actual functionality or processes that might be associated with the Specified Processing. In practice however such functionality or processes might include, without limitation, obtaining, holding, storing, displaying, transferring, replicating, or the processing of Personal Data Items in any other way. It is assumed herein that the Generic SCPPD will be integrated with any additional functionality actually required to achieve the Specified Processing.

2.2 LOG-ON AND CONSENT FOR SPECIFIED PROCESSING



2.2.1 Overview

This function is the first accessed when the Data Subject visits the website. The function is used to identify the Data Subject to the system and to gain the Data Subject's consent over the web for the Specified Processing of Personal Data Items. The Data Controller can also log on to the system through this function.

When anyone signs onto the system, their username and password are validated against the **UserName** and **UserPassword** values on the USER table. If the **ForcePasswordChange** flag is set for the User, the user will be required to change his/ her password. On successful validation of the username and password, if the User is identified as a Data Subject, determined by the value of the **UserDataSubject** flag on the User table, the **UserID** will be used to determine the Data Subject record.

If the **DataSubjectSpecifiedProcessingAgreed** flag is not set (which will be the case when the Data Subject visits the site for the first time), the Data Subject will be presented with an explicit specification of all processing that is to be performed (the Specified Processing) on all Personal Data Items, and will be informed that Personal Data Items are to be viewable by the Data Controller and by the Data Subject. The description of the Specified Processing will be taken from the **SpecifiedProcessingText** (held on the SPECIFIED PROCESSING table) that will be entered and maintained by the Data Controller (see 2.5, NEW SPECIFIED PROCESSING OF PERSONAL DATA ITEMS). If the Data Subject does not agree to this processing, he or she will *not* be allowed to proceed any further, and an e-mail will be generated and sent to the Data Controller so that the Data Subject can be contacted if necessary and the issue resolved. If the Data Subject does consent, then the **Consent** field (held on the PERSONAL DATA ITEM table) is updated to Y for all Personal Data Items for that Data Subject, the **DataSubjectSpecifiedProcessingAgreed** (held on the DATA SUBJECT table) is set to Y for that Data Subject and the **DataSubjectSpecifiedProcessingAgreedDate** (held on the DATA SUBJECT table) is set to the current date.

On subsequent visits to the website, if the Data Subject has previously agreed to the Specified Processing (as indicated by the **DataSubjectSpecifiedProcessingAgreed** flag for the Data Subject) and the Specified Processing details have not changed in the mean time, they will not be required to agree to the same conditions again though they will need to log on with their username and password.

2.2.2 Database & Tables

The databases used during this business event are:

- USER table
- SPECIFIED PROCESSING table
- DATA SUBJECT table

2.2.3 Fields on the Screen

The contents of this screen are:

Log-on-Username: uniquely identifies the user and is checked against the USER table. It is a maximum of 20 alphanumeric characters.

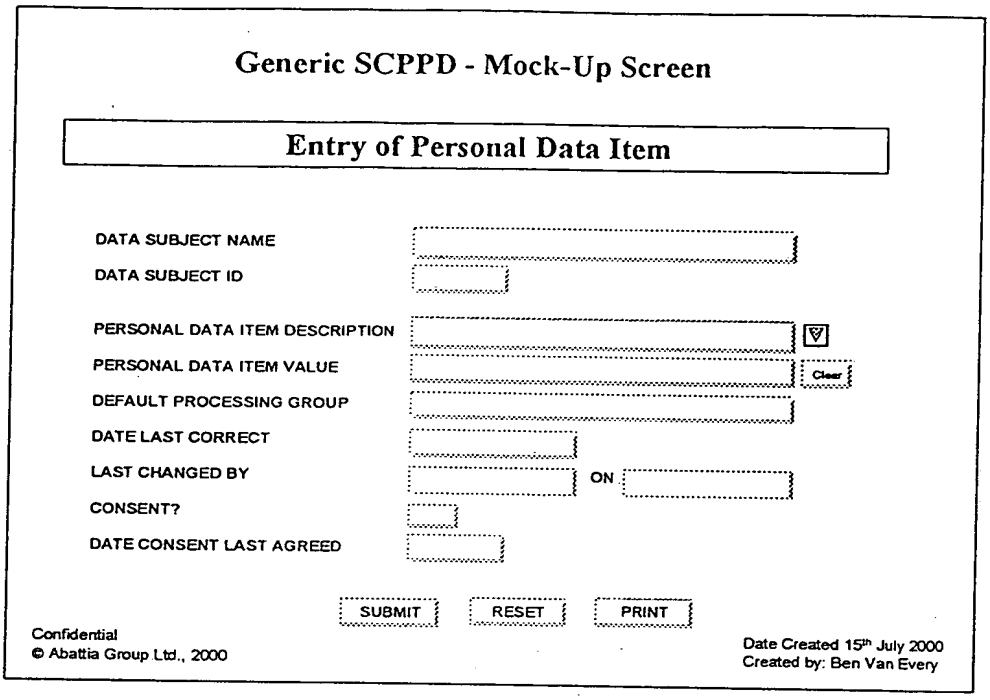
Log-on-Password: when entered, is hidden from the user and is encrypted when held on the database. It is checked against the USER table in conjunction with the username.

Log-on-Specified-Processing: an explicit specification of all processing that is to be performed on the Personal Data Items, including that Personal Data Items are to be viewable by the Data Controller and by the Data Subject. This is sourced from the **SpecifiedProcessingText** value in the SPECIFIED PROCESSING table.

Log-on-IAgreeToSpecifiedProcessing: on clicking this input button, the Data Subject consents to the Specified Processing in relation to the Personal Data Items, and this process updates the **Consent** field in all records on the PESRONAL DATA ITEM table for the Data Subject to Y. By agreeing to the Specified Processing the Data Subject is then able to view each individual Personal Data Item separately through 2.3, ENTRY OF PERSONAL DATA ITEM, and, if he/ she so wishes, to amend the **Consent** field value for logical groups of Personal Data Items to N. (Note, that by amending this **Consent** value for any of the Data Subject's Personal Data Items, they are in effect denying themselves access to the website until they agree to the Specified Processing again).

Log-on-IDoNotAgreeToSpecifiedProcessing: on clicking this input button, the Data Subject has declined the Specified Processing and the **DataSubjectSpecifiedProcessingAgreed** flag will remain as N. All **Consent** field values for all Personal Data Items will remain as N also. An e-mail will be generated and sent to the Data Controller detailing this declination event. The Data Subject will not be permitted any further access to the website beyond this Log-on page.

2.3 ENTRY OF PERSONAL DATA ITEM



2.3.1 Overview

This function presents the basic information regarding a Data Subject, and allows the Data Subject to inform the Data Controller regarding a Personal Data Item relating to the Data Subject. Additionally, this function will allow the Data Controller to make available to the Data Subject over the Internet all Personal Data Items held relating to that Data Subject, and to gain confirmation from each Data Subject as to the integrity of the data. Furthermore, the screen allows for the Data Subject to view whether he or she has consented to the Specified Processing, and to alter this election, if they so wish.

To Change Existing Information: the Data Subject selects a Personal Data Item Description from a drop-down list of those available (list contents are taken from the DATA ITEM table). The Data Subject overtypes with the new information in the Personal Data Item field and the form is submitted. If the Function Notification record indicates that notification is required for the amended Data Item, any change to the data held on this page is detailed in an e-mail automatically sent to the Data Controller.

To Add New Information: the Data Subject selects a Personal Data Item Description from the drop-down list of those available. The new Personal Data Item value information is entered into the Personal Data Item Value field and the form is submitted.

To Remove Information: the Data Subject selects the Personal Data Item from the drop-down list of those available. The Data Subject then clears the Personal Data Item Value by clicking on the Clear button or by deleting the contents, and the form is submitted.

2.3.2 Database & Tables

The information on this screen is held on the PERSONAL DATA ITEM table. Other databases used are:

- FUNCTION NOTIFICATION table
- USER table
- BUSINESS FUNCTION ACCESS table

- DATA ITEM table
- DATA SUBJECT table

2.3.3 Tracking Changes

If the Data Subject changes the Personal Data Item value, the FUNCTION NOTIFICATION table is interrogated to determine whether the Data Controller wants to be notified about the change. If the Functional Notification flag for the Data Item is set then the UserID (held on the FUNCTION NOTIFICATION table) is retrieved and used to find the appropriate UserDataControllerE-mail address (held on the USER table), to which an automatically generated e-mail is sent e-mailwith the following message in the Subject:

<Data Subject Name>, ID: <Data Subject ID> changed their <Personal Data Item Description> from ****** to ######## on DD/MM/YYYY at HH:MM:SS.

2.3.4 Fields on the Screen

PDI-Data-Subject-ID: This is the unique identifier assigned to this Data Subject by the Data Controller. It is a maximum of 20 characters numeric.

PDI-Data-Subject-Name: This is the name of the Data Subject, which is initially entered by the Data Controller. In the instance that the Personal Data Item is the Data Subject's name, this field could instead be some other identifier of the Data Subject. It is a maximum of 100 alphanumeric characters long.

PDI-Personal-Data-Item-Value: This is an item of personal data relating to the Data Subject, which might include, without limitation, any of the following; name details, contact details, family details, health details, financial details, lifestyle details, life stage details, life events details, demographic details, any details relating to the Data Subject's relationship to the Data Controller, or any other such personal data. This is a maximum 400 alphanumeric character field.

PDI-Personal-Data-Item-Description: This identifies the Data Item to which the Personal Data Item Value refers. The Data Subject can request a display of a specific item such as "Address" by selecting the Address description from the drop-down list. On selecting a description, the Personal Data Item Value held for that description against the Data Subject is displayed.

PDI-Default-Processing-Group: This specifies how a Data Item is to be Processed in the period prior to explicit consent for processing being obtained from the Data Subject, and as detailed in the Specified Processing. This classification allows for the Data Controller to take into account different processing requirements and restrictions that might apply to particular types of data, such as the differing treatments of so-called "sensitive" and "non-sensitive" data under the UK's 1998 Data Protection Act.

PDI-Clear: The Personal Data Item Value for any given Data Item can be cleared out using this button. The form is then submitted to process the removal of data.

PDI-Date-Last-Correct: This field can be updated directly by the Data Subject, or will be set automatically after any view or change of the data item by the Data Subject. This is a date and time displayed in the format DD/MM/YYYY HH:MM:SS.

PDI-Last-Changed-By / On: This field representes the date of the last amendment (displayed in the format DD/MM/YYYY HH:MM:SS) and the username of the last person who updated this Personal Data Item Value (maximum 20 characters alphanumeric).

PDI-Consent: This field indicates that the Data Subject consents to the Specified Processing of the Personal Data Item. The Data Subject can withdraw consent for such usage by changing the contents of this field. If the Data Subject withdraws consent for the Specified Processing of this Personal Data Item, further access to the Generic SCPPD will be withdrawn by setting the **DataSubjectSpecifiedProcessingAgreed** to N (see 2.2, LOG-ON AND CONSENT FOR SPECIFIED PROCESSING), whereupon the Log-on page (see 2.2, LOG-ON AND CONSENT FOR SPECIFIED

PROCESSING) will be the only screen accessible to the Data Subject, and an e-mail will be sent to the Data Controller so that the Data Subject can be contacted if necessary and the issue resolved.

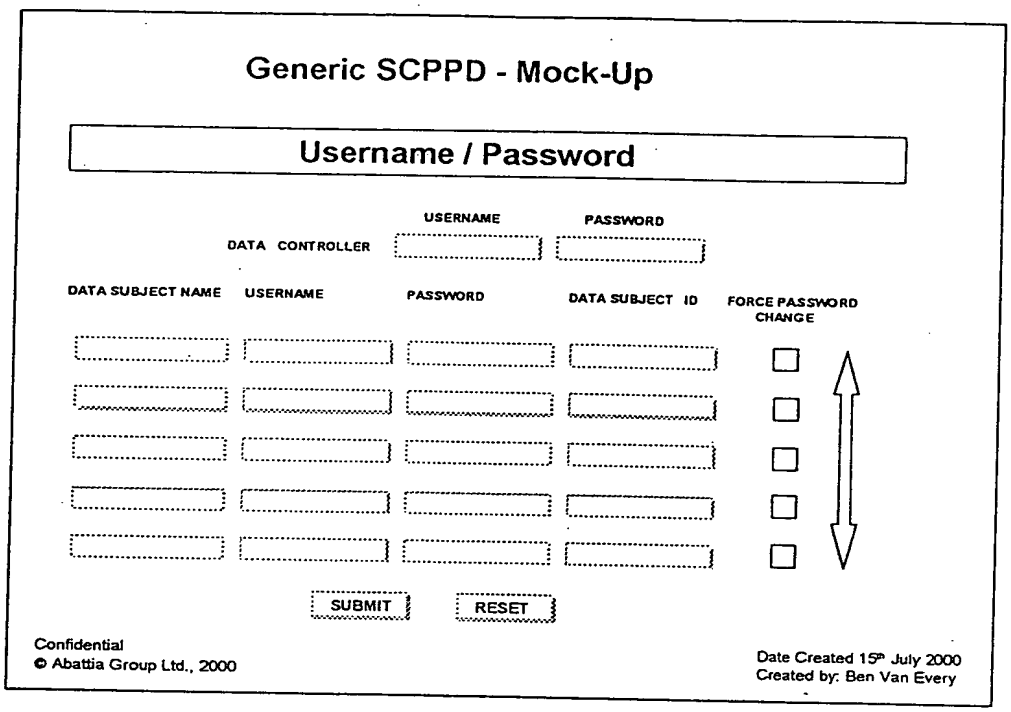
PDI-Consent-Date-Agreed: This is the date that the Data Subject last provided their consent for Specified Processing (see 2.2, LOG-ON AND CONSENT FOR SPECIFIED PROCESSING). This is displayed as a date and time in the format DD/MM/YYYY HH:MM:SS. If the Data Subject subsequently alters any election in respect of consent for Specified Processing, this field will reflect that date at which this alteration was made. Effectively, all Consent dates will be that of the date that Specified Processing agreement was made.

PDI-Submit: By clicking this button the changes to the Personal Data Item are saved to the database.

PDI-Reset: Any changes that were 'in-progress' will be discarded and the page returned to its original state by clicking this button.

PDI-Print: This allows a report to be printed based upon the Personal Data Item being viewed.

2.4 USERNAME/PASSWORD MAINTENANCE



2.4.1 Overview

Only the Data Controller can access this function, which controls access to the system on an individual Data Subject level. It also provides the Data Controller with the ability to amend his or her own password.

2.4.2 Database & Tables

This information is held on the USER table. The other table used is:

- DATA SUBJECT table

2.4.3 Fields on the Screen

UPT-Data-Controller-Username: This is the Data Controller's username, used to sign onto the system, which can be changed via this page. It is a maximum of 20 alphanumeric characters in length. The Data Controller in this table initially assigns it, together with a password.

UPT-Data-Controller-Password: This is the Data Controller's password, which can be changed via this page.

UPT-Data-Subject-Name: This is the name of the Data Subject, which is obtained from the DATA SUBJECT table using the Data-Subject-ID as the key. It is a maximum of 100 alphanumeric characters in length.

UPT-Username: This is the Data Subject's username, used to sign onto the system, which can be changed via this page. It is a maximum of 20 alphanumeric characters in length. It is originally assigned, together with a password, by the Data Controller in this table, and is then related to a series of business events through the Business Function Access page (see 2.9, BUSINESS FUNCTION ACCESS).

UPT-Password: This is the Data Subject's password, which can be changed via this page. It is shown on this page in its unencrypted form.

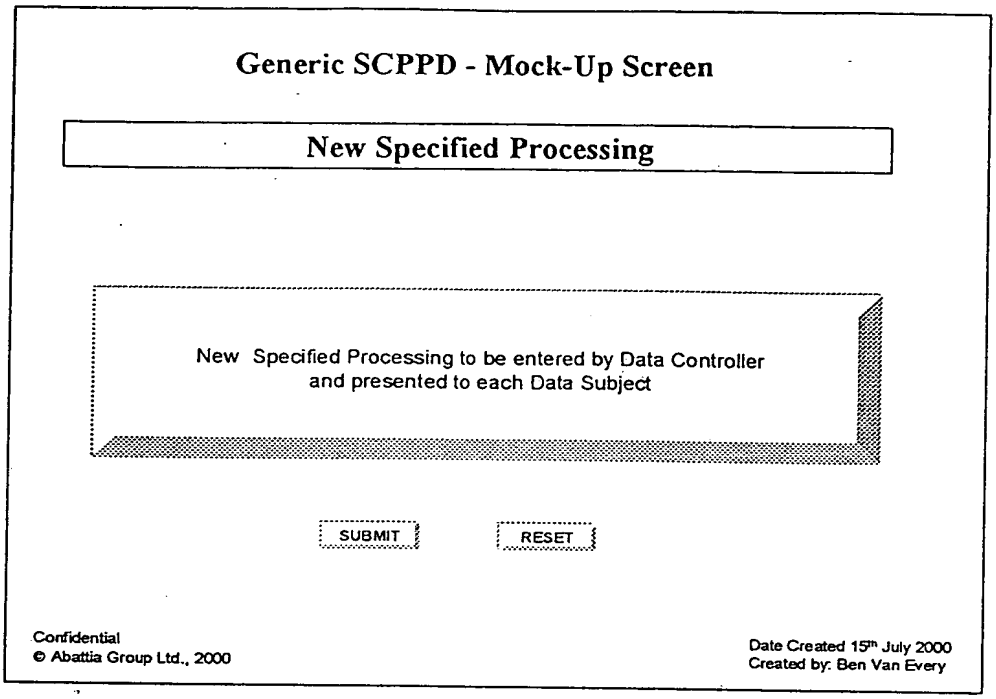
UPT-Data-Subject-ID: This is the unique identifier, generated by the system, and assigned to this Data Subject.

UPT-Force-Password-Change: This checkbox allows the Data Controller to set the ForcePasswordChange flag for the Data Subject. This will require the Data Subject to change their password when they next log on to the site.

UPT-Submit: By clicking this button the changes to the Username and Password details are saved to the database.

UPT-Reset: By clicking this button, any changes that were 'in-progress' will be discarded and the page returned to its original state.

2.5 NEW SPECIFIED PROCESSING OF PERSONAL DATA ITEMS



2.5.1 Overview

Whenever the Data Controller changes the nature of the Specified Processing to be applied to Data Items, the Data Controller is required to seek consent for the New Specified Processing from the Data Subject. This function will allow the Data Controller to establish a new description of the Specified Processing of the Data Items. By submitting a New Specified Processing text, the **DataSubjectSpecifiedProcessingAgreed** flag and date are reset for each Data Subject. When the Data Subjects next sign onto the system, they will be required to consent to the new Specified Processing as a condition for using the system (see 2.2, LOG-ON AND CONSENT FOR SPECIFIED PROCESSING).

2.5.2 Database & Tables

The new description of the Specified Processing is held on the SPECIFIED PROCESSING table. The other table used is:

- DATA SUBJECT table

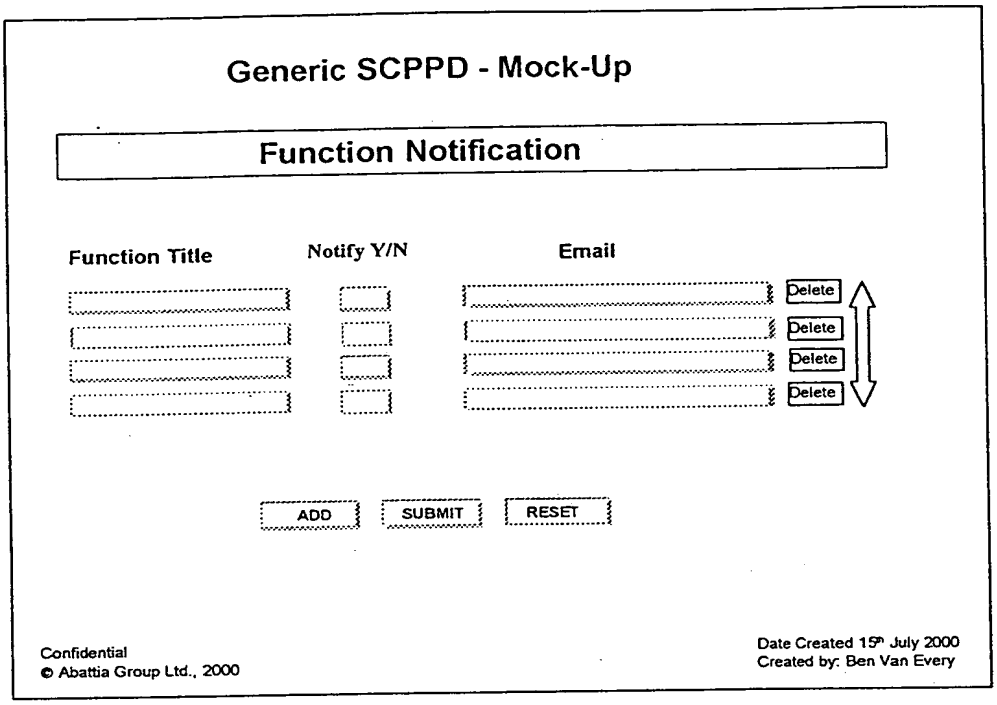
2.5.3 Fields on the Screen

SP-New-Description: This contains the new description of Specified Processing that will be displayed for the Data Subject to give their consent when they next log on.

SP-Submit: This button submits the change to the Specified Processing to the SPECIFIEDPROCESSING table and sets the **DataSubjectSpecifiedProcessingAgreed/Date** to N and NULL respectively.

SP-Reset: By clicking this button, any changes that were 'in-progress' will be discarded and the page returned to its original state.

2.6 FUNCTION NOTIFICATION



2.6.1 Overview

This function allows the Data Controller to control who, if anyone, is informed about changes to Personal Data Items. A change by a Data Subject (not by the Data Controller) will cause a standard e-mail to be generated and automatically sent to the e-mail address of the specified administrator.

2.6.2 Databases and Tables

This information is stored on the FUNCTION NOTIFICATION table.

The other table used is:

- DATA ITEM table

2.6.3 Fields on the Screen

FN-Notify: This checkbox indicates whether the Data Controller is going to be notified by e-mail when the Data Subject changes the respective Personal Data Item.

FN-E-mail: This is the e-mail address to which the e-mail is to be sent. This is a 30 character alphanumeric field.

FN-Function-Title: This indicates the function to which the Function Notification setting applies.

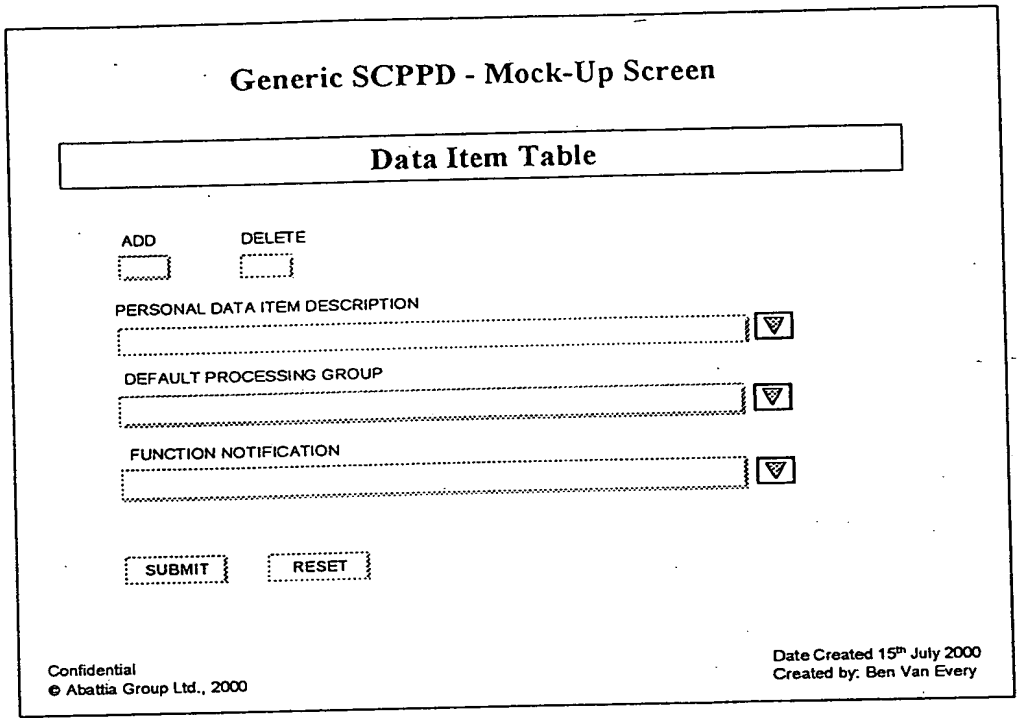
FN-Add: This button allows the Data Controller to add a new Function Notification to the FUNCTION NOTIFICATION table.

FN-Delete: This allows the Data Controller to delete a Function Notification providing that the Function Notification is not referenced by any Data Item on the database.

FN-Submit: By clicking this button the changes to the Function Notification parameters are saved to the database.

FN-Reset: By clicking this button, any changes that were 'in-progress' will be discarded and the page returned to its original state.

2.7 DATA ITEM PAGE



2.7.1 Overview

This function allows the Data Controller to establish the standard Data Item Descriptions and to specify how Personal Data Items with these Data Item Descriptions are to be Processed in the period prior to explicit consent for processing being obtained from the Data Subject, i.e. the period between the data "going live" on the database following entry by the Data Controller and the first time it is verified by the Data Subject. This classification allows the Data Controller to account for different processing requirements or restrictions that might apply to particular types of data, such as the differing treatments of so-called "sensitive" and "non-sensitive" data under the UK's 1998 Data Protection Act.

When a new Data Item Description is added, the details are stored on the DATA ITEM table.

A Data Item Description cannot be removed if it is used on the PERSONAL DATA ITEM table.

This function also allows the Data Controller to specify which Function Notification details should be associated with a given Data Item.

2.7.2 Database & Tables

This is stored in the DATA ITEM table. Other tables used are:

- PERSONAL DATA ITEM table
- DEFAULT PROCESSING GROUP table
- FUNCTION NOTIFICATION table

2.7.3 Fields on the screen

DI-Add: This allows the Data Controller to add a new Personal Data Item Description. The Personal Data Item Description drop-down box will be enabled so that the Data Controller can enter the new Data Item description. The association to a Default Processing Group is also made.

DI-Delete: This allows the Data Controller to delete a Data Item Description from the table provided there are currently no Personal Data Items on the PERSONAL DATA ITEM table associated with it.

DI-Persqnal-Data-Item-Description: This is the description of the Data Item, and will be no longer than 20 alphanumeric characters.

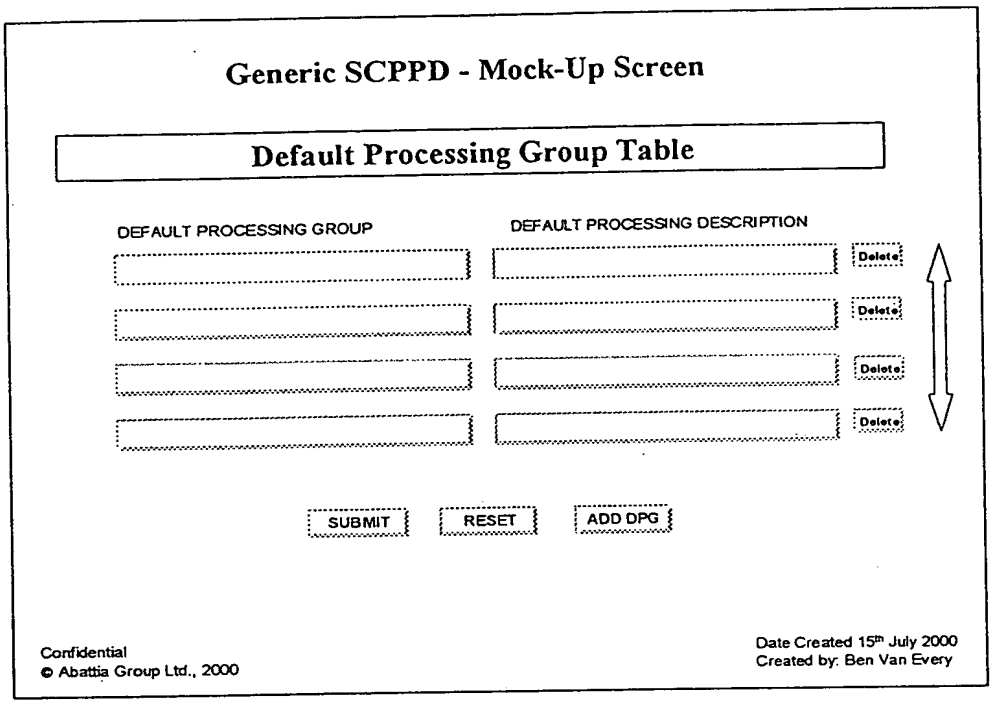
DI-Default-Processing-Group: This specifies how Data Items with this Data Item Description are to be Processed prior to explicit consent for processing being obtained from the Data Subject, i.e. the period between the data "going live" on the database following entry by the Data Controller and the first time it is verified by the Data Subject. This classification allows for the Data Controller to account for different processing requirements that might apply to particular types of data, such as the differing treatments of so-called "sensitive" and "non-sensitive" data under the UK's 1998 Data Protection Act.

DI-Function-Notification: This allows the Data Controller to indicate which Function Notification detail is to be associated with the Data Item.

DI-Submit: By clicking this button the additions, changes or deletions are processed on the DATA ITEM table.

DI-Reset: By clicking this button any changes that were 'in-progress' will be discarded and the page returned to its original state.

2.8 DEFAULT PROCESSING GROUP PAGE



2.8.1 Overview

This function allows the Data Controller to maintain the Default Processing Groups and to establish what Default Processing will be associated with each Default Processing Group. When a new Default Processing Group is added, the details are added clicking this button the DEFAULT PROCESSING GROUP table.

A Default Processing Group cannot be deleted if it is used on the DATA ITEM table.

As the Generic SCPPD is intended as a "generic" engine, no description is given herein of actual functionality or processes that might be associated with the Default Processing. In practice however such functionality or processes might include, without limitation, obtaining, holding, storing, displaying, transferring, replicating, or the processing of Personal Data Items in any other way. It is assumed herein that the Generic SCPPD will be integrated with any additional functionality actually required to achieve the Specified Processing.

2.8.2 Database & Tables

This is stored in the DEFAULT PROCESSING GROUP table. The other table used is:

- DATA ITEM table

2.8.3 Fields on the Screen

DPG-Default-Processing-Group: This is the name of the Default Processing Group, and will be no longer than 20 alphanumeric characters.

DPG-Default-Processing-Description: This is the Default Processing associated with the Default Processing Group.

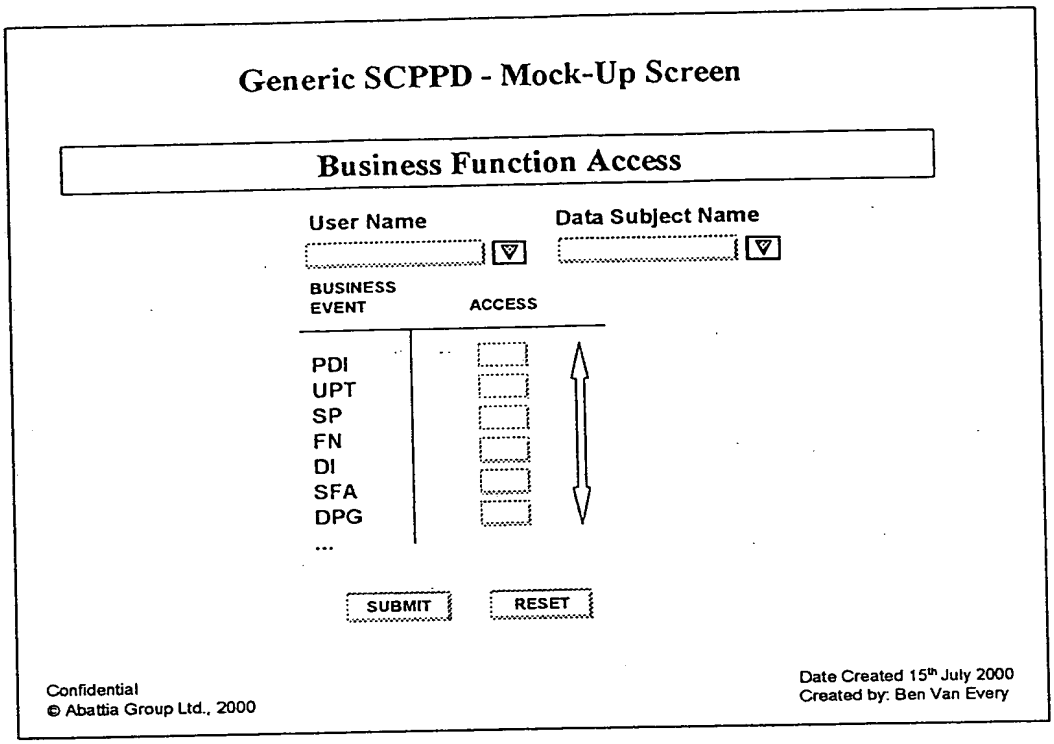
DPG-Add-DPG: This button allows the Data Controller to add a new Default Processing Group and will add the details to the DEFAULT PROCESSING GROUP table.

DPG-Delete: This allows the Data Controller to delete a Default Processing Group from the table provided there are currently no Data Items on the DATA ITEM table associated with it.

DPG-Submit: By clicking this button the additions, changes or deletions are processed on the DEFAULT PROCESSING GROUP table.

DPG-Reset: By clicking this button any changes that were 'in-progress' will be discarded and the page returned to its original state.

2.9 BUSINESS FUNCTION ACCESS



2.9.1 Overview

This function allows the Data Controller to specify which business events (i.e. functional activity generally related to a screen) can be accessed by the Users. This covers all possible functions within the system, with the exception of the Log-on function, which is always accessible to all users (see 2.2, LOG-ON AND CONSENT FOR SPECIFIED PROCESSING). The list of Business Events available is built from the BUSINESS FUNCTION table using the **BusinessFunctionTitle.** Access can be View or Update.

2.9.2 Database & Tables

This is stored in the BUSINESS FUCTION ACCESS table.

The other tables used are:

- USER table
- DATA SUBJECT table

2.9.3 Fields on the Screen

BFA-UserName: This is a drop-down list of usernames from the User table. Selection of a username brings up the Business Event Access values for that User.

BFA-Data-Subject-Name: This is a drop-down list of Data Subject Names from the DATA SUBJECT table that will be kept in line with the username drop-down list. There may be usernames for which there are no Data Subject Names e.g. Data Controllers.

BFA-PDI: This field records whether the User is to have access to the Entry of Personal Data function (see 2.3, ENTRY OF PERSONAL DATA ITEM).

BFA-UPT: This field records whether the User is to have access to the Username/Password function (see 2.4, USERNAME/PASSWORD).

BFA-SP: This field records whether the User is to have access to the New Psecified Processing of Personal Data Items function (see 2.5, NEW SPECIFIED PROCESSING OF PERSONAL DATA ITEMS).

BFA-FN: This field records whether the User is to have access to Function Notification function (see 2.6, FUNCTION NOTIFICATION).

BFA-DI: This field records whether the User is to have access to the Data Item function (see 2.7, DATA ITEM PAGE.)

BFA-DPG: This field records whether the User is to have access to the Default Processing Group function (see 2.8, DEFAULT PROCESSING GROUP PAGE).

BFA-BFA: This field records whether the User is to have access to the Business Function Access function (see 2.9, BUSINESS FUNCTION ACCESS).

BFA-...: This field records whether the User is to have access to other Business Functions as recorded on the BUSINESS FUNCTION table.

BFA-Submit: By clicking this button the changes are processed on the BUSINESS FUNCTION ACCESS table.

BFA-Reset: By clicking this button any changes that were 'in-progress' will be discarded and the page returned to its original state.

2.10 REPORT

2.10.1 Overview

A paper or e-mail report can be produced by the system. The reports can be printed and sent or e-mailed to the Data Subject to have the Data Subject verify the integrity of the Personal Data Item, by letting the Data Subject check the details held and return any corrections. Reports can be produced in such a way that they can be e-mailed as an attachment.

2.10.2 Source of information

The following table provides the source of this information:

- PERSONAL DATA ITEM table

2.10.3 Fields printed on the report.

DATA SUBJECT PERSONAL DATA ITEM

Printed by: <username> on DD/MMM/YYYY

NAME	**<PDI-Data-Subject-Name>**
DATA SUBJECT ID NUMBER	**<PDI-Data-Subject-ID>**
Description of Specified Processing:	**<SP-New-Description>**

[There follows a list of all Personal Data Items relating to this Data Subject, as follows....]

#1

Personal Data Item Description:	**<PDI-Personal-Data-Item Description>**
Personal Data Item:	**<PDI-Personal-Data-Item Value>**
Consent Given?	**<PDI-Consent>**
Date Consent Given	**<PDI-Consent-Date-Agreed>**
Default Processing Group	**<PDII-Default-Processing-Group>**
Default Processing	**<DPG-Default-Processing>**
Details were correct on	**<PDI-Date-Last-Correct>**
Last changed by	**<PDI-Last-Changed-By>** On **<PDI-Last-Changed-On>**

#2, etc...

3. FUNCTIONAL SPECIFICATION

3.1 LOG-ON AND CONSENT FOR SPECIFIED PROCESSING
(See 2.2, LOG-ON AND CONSENT FOR SPECIFIED PROCESSING)

Overview
Log-on and Consent for Specified Processing allows a user to connect to the site and to provide consent for Data Items to be processed in a specified manner.

Primary User
Data Controller
Data Subject

Starting Point
When a user navigates to the Log-on portal of the website.

Ending Point
When a Log-on request has been completed.

Measurable Result
The user is eith granted or denied access to the system beyond the Log-on page.

Flow of events
The username and password of a user is referenced against the USER table.

Where the Username entered corresponds to that of a Data Controller and the password is valid, the **DataSubjectSpecifiedProcessingAgreed** field is ignored.

Where the username entered corresponds to a Data Subject and the password is valid, and if the **DataSubjectSpecifiedProcessingAgreed** field indicates agreement to the Specified Processing presented at Log-on, the **DataSubjectSpecifiedProcessingAgreedDate** field on the DATA SUBJECT table is updated with the current date and the **Consent** field on all PERSONAL DATA ITEM records is set to Y for the Data Subject. However, I the Data Subject declines the Specified Processing presented at Log-on, the Data Subject user will be informed that they are not able to continue any further into the website and an e-mail will be automatically generated and sent to the Data Controller indicating that this is the case. The **DataSubjectSpecifiedProcessingAgreed** flag will be set to N and the **DataSubjectSpecifiedProcessingAgreedDate** will be set to NULL. All Consent flags on all PERSONAL DATA ITEM records for the Data Subject will also be set to N.

Where a user attempts to log-on to the website and the username provided indicates that the **Force-Password-Change** flag is set, the user must change their password before any further processing can continue.

When the user successfully logs on to the system, a unique SessionID is generated by the system and written to the **UserSessionID** field, and the **UserLastAccess** field is updated with the current timestamp. Both of these fields are held on the USER table.

The SessionID is passed from page to page as the user navigates through the system, and serves both to identify the user to the system, and to force a user to log-on again if they have been inactive for a certain length of time.

Alternative flow of events
If the username provided does not match a reference in the USER table, or the username and password combination do not match an entry in that table, the Log-on attempt will fail and the user will be informed of the failure and prevented from progressing beyond the Log-on page.

3.2 SEARCH PERSONAL DATA ITEM DATABASE
(See 2.3, ENTRY OF PERSONAL DATA ITEM)

Overview
To interrogate the PERSONAL DATA ITEM table based upon the name of the Data Subject and the Personal Data Item Description and return the Personal Data Item Value.

Primary User
Data Controller
Data Subject

Starting Point
When the Data Controller chooses to perform a PERSONAL DATA ITEM table search, or when a Data Subject accesses the Entry of Personal Data Item function.

Ending Point
When the search request has been completed.

Measurable Result
A result set containing a Data Subject's name, the Personal Data Item Description, and Personal Data Item Value is returned.

Flow of events
Check that the SessionID supplied is valid and current, and establish authorisation to perform this function (Check Authority).

The Data Controller enters the name of a Data Subject, (entered automatically if the functionis being access by the Data Subject).

The Data Controller or the Data Subject selects the Personal Data Item Description from a drop-down list.

It is possible to use a wildcard within the Data Subject field, where the wildcard character will be an asterisk and can only be used at the end of a text string.

The search is performed using the DISPLAY PERSONAL DATA ITEM SEARCH RESULTS function, and the results are presented to the user.

The function will break the list of details into manageable chunks, and provide controls to allow the user to page backwards and forwards between them, or to jump to any other chunk.

Alternative flow of events
The user is denied access due to lack of authority, or is referred back to theLog-on page because their SessionID is invalid or has expired.

3.3 DISPLAY PERSONAL DATA ITEM SEARCH RESULTS
(See 2.3, ENTRY OF PERSONAL DATA ITEM)

Overview
To execute a search and display the resulting Data Subject and Personal Data Item as supplied by the SEARCH PERSONAL DATA ITEM DATABASE function.

Primary User
Data Controller
Data Subject

Starting Point
When a serach is requested on the PERSONAL DATA ITEM table using the SEARCH PERSONAL DATA ITEM DATABASE function.

Ending Point
When the search has been executed and the resulting Data Subject name and Personal Data Item have been returned.

Measurable Result
A result set containing a Data Subject's name, the Personal Data Item Description, and Personal Data Item Value is returned.

Flow of events
Check that the SessionID supplied is valid and current, and establish authorisation to perform this function (Check Authority).

The search is executed, and the resulting result set is returned.

Alternative flow of events
As a result of the search criteria supplied, no results are returned, in which case the PDI-Personal-Data-Item field (see 2.3, ENTRY OF PERSONAL DATA ITEM) remains blank, and is displayed as such.

Or the user is denied access due to lack of authority, or is referred back to theLog-on page because their SessionID is invalid or has expired.

3.4 PERSONAL DATA ITEM
(See 2.3, ENTRY OF PERSONAL DATA ITEM)

3.4.1 View

Overview
This enables the Data Controller to view the personal data item relating to a Data Subject. It also allows the Data Subject to view his or her own Personal Data Items.

Primary User
Data Controller
Data Subject

Starting Point
When the user selects a specific Data Subject's Personal Data Item to view.

Ending Point
When the requested information has been presented to the user.

Measurable Result
The requested information has been presented to the user.

Flow of events
Check that the SessionID supplied is valid and current, and establish authorisation to perform this function (Check Authority).

The selected Data Subject's details are displayed to the user.

Where the Data Subject has viewed this information, the date in the PDI-Date-Last-Correct field is set to today's date.

The Data Controller can set the PDI-Date-Last-Correct field to confirm that they have verification from the Data Subject of the integrity of the Data Item.

Alternative flow of events
The user is denied access due to lack of authority, or is referred back to theLog-on page because their SessionID is invalid or has expired.

3.4.2 Add

Overview
This enables the user to add a Personal Data Item relating to a Data Subject.

Primary User
Data Controller
Data Subject

Starting Point
When the user enters new information for a Data Subject and submits the data.

Ending Point
When the information has been validated and processed by the system, and the user is informed of the success or failure of the operation.

Measurable Result
A Data Subject's Personal Data Item Value has been added for a Data Subject.

Flow of events
Check that the SessionID supplied is valid and current, and establish authorisation to perform this function (Check Authority).

The Data Controller can explicitly set the PDI-Date-Last-Correct field to confirm that they have verification from the Data Subject of the integrity of the Data Item.

If the addition has been applied by the Data Subject the Check IF DATA CONTROLLER NOTIFICATION REQUIRED function will be called.

Alternative flow of events
Data entered fails validation, in which case the user is informed of the issue(s) and is invited to re-try the update after correction.

Or, the user is denied access due to lack of authority, or is referred back to theLog-on page because their SessionID is invalid or has expired.

3.4.3 Update

Overview
This enables the Data Controller to update the Personal Data Item relating to a Data Subject. It also allows the Data Subject to verify and/or update his or her own information.

Primary User
Data Controller
Data Subject

Starting Point
When the user makes amendments to the Data Subject's Personal Data Item and submits the data.

Ending Point
When the information has been validated and processed by the system, and the user is informed of the success or failure of the operation.

Measurable Result
A Data Subject's Personal Data Item is updated.

Flow of events
Check that the SessionID supplied is valid and current, and establish authorisation to perform this function (Check Authority).

Changes will be confirmed with the user before being applied. All data should be validated both prior to confirmation and prior to update, and the user notified of any errors and given the opportunity to correct them.

Before applying changes to the database, it should be checked to ensure that another user has not updated the same data in the period between this user first viewing it and subsequently making a change. Where this is the case the update should be refused, and the user should be returned to the update screen showing the latest information from the database.

Where the Data Subject has viewed this information, the date in the PDI-Date-Last-Correct field is set to today's date.

The Data Controller can set the PDI-Date-Last-Correct field to confirm that they have verification from the Data Subject of the integrity of the Data Item.

If the change has been applied by the Data Subject the Check IF DATA CONTROLLER NOTIFICATION REQUIRED function will be called.

Alternative flow of events
Data entered fails validation, in which case the user is informed of the issue(s) and is invited to re-try the update after correction.

Or, the user is denied access due to lack of authority, or is referred back to theLog-on page because their SessionID is invalid or has expired.

3.4.4 Print

Overview
This enables the Data Controller to print a report of the Personal Data Item relating to the Data Subject.

Primary User
Data Controller

Starting Point
When the user presses the print button on the Entry of Personal Data page (see 2.3, ENTRY OF PERSONAL DATA ITEM).

Ending Point
When the report has been printed.

Measurable Result
A Data Subject's Personal Data Item report has been produced (see 2.10, REPORT).

Flow of events
Check that the SessionID supplied is valid and current, and establish authorisation to perform this function (Check Authority).

Print the report based upon the selected Personal Data Item.

Alternative flow of events
The user is denied access due to lack of authority, or is referred back to theLog-on page because their SessionID is invalid or has expired.

3.5 MAINTAIN FUNCTION NOTIFICATIONS
(See 2.6, FUNCTION NOTIFICATION)

3.5.1 View

Overview
This enables the Data Controller to view the Function Notification settings.

Primary User
Data Controller

Starting Point
When the user elects to view Function Notifications.

Ending Point
When the information has been presented to the user.

Measurable Result
The Function Notification information is presented to the user.

Flow of events
Check that the SessionID supplied is valid and current, and establish authorisation to perform this function (Check Authority).

The Function Notification Title, the Notify setting and the E-mail Address of the administrator to be e-mailed are presented to the user.

The function will break the list of details into manageable chunks, and provide controls to allow the user to page backwards and forwards between them, or to jump to any other chunk.

Alternative flow of events
The user is denied access due to lack of authority, or is referred back to theLog-on page because their SessionID is invalid or has expired.

3.5.2 Add

Overview
This enables the Data Controller to add a Function Notification title, setting, and e-mail address.

Primary User
Data Controller

Starting Point
When the user enters new information for a Function Notification.

Ending Point
When the information has been validated and processed by the system, and the user is informed of the success or failure of the operation.

Measurable Result
A Function Notification is been added.

Flow of events
Check that the SessionID supplied is valid and current, and establish authorisation to perform this function (Check Authority).

The Function Notification Title is entered. The Notify setting must be Y or N, and the E-mail address for

the administrator to be notified is entered before being submitted. On validating correctly, the data will be written to the FUNCTION NOTIFICATION table.

Alternative flow of events
Data entered fails validation, in which case the user is informed of the issue(s) and is invited to re-try the update after correction.

Or, the user is denied access due to lack of authority, or is referred back to theLog-on page because their SessionID is invalid or has expired.

3.5.3 Update

Overview
This enables the Data Controller to update the Function Notification settings.

Primary User
Data Controller

Starting Point
When the user elects to update the current Function Notification information.

Ending Point
When the information has been validated and processed by the system, and the user is informed of the success or failure of the operation.

Measurable Result
The Function Notification records are updated.

Flow of events
Check that the SessionID supplied is valid and current, and establish authorisation to perform this function (Check Authority).

Changes will be confirmed with the user before being applied. All data should be validated both prior to confirmation and prior to update, and the user notified of any errors and given the opportunity to correct them.

Before applying changes to the database, it should be checked to ensure that another user has not updated the same data in the period between this user first viewing it and subsequently making a change. Where this is the case the update should be refused, and the user should be returned to the update screen showing the latest information from the database.

Alternative flow of events
Data entered fails validation, in which case the user is informed of the issue(s) and is invited to re-try the update after correction.

Or, the user is denied access due to lack of authority, or is referred back to theLog-on page because their SessionID is invalid or has expired.

3.5.4 Delete

Overview
This enables the user to delete Function Notification records.

Primary User
Data Controller

Starting Point
When the user chooses to delete Function Notification details.

Ending Point
When the information has been applied to the database or has been cancelled due to failure.

Measurable Result
The requested deletions are applied.

Flow of events
Check that the SessionID supplied is valid and current, and establish authorisation to perform this function (Check Authority).

Delete the selected Function Notification record(s) from the database, providing that they are not currently in use by Data Item records.

Alternative flow of events
The deletion fails, in which case the user is informed of the issue(s).

Or the user is denied access due to lack of authority, or is referred back to theLog-on page because their SessionID is invalid or has expired.

3.6 MAINTAIN BUSINESS FUNCTION ACCESSES
(See 2.9, BUSINESS FUNCTION ACCESS)

3.6.1 View

Overview
This enables the Data Controller to view the Business Function Accesses.

Primary User
Data Controller

Starting Point
When the user elects to view Business Function Accesses.

Ending Point
When the information has been presented to the user.

Measurable Result
The Business Function Accesses information is presented to the user.

Flow of events
Check that the SessionID supplied is valid and current, and establish authorisation to perform this function (Check Authority).

The Business Function Accesses are presented to the user.

The function will break the list of details into manageable chunks, and provide controls to allow the user to page backwards and forwards between them, or to jump to any other chunk.

Alternative flow of events
The user is denied access due to lack of authority, or is referred back to theLog-on page because their SessionID is invalid or has expired.

3.6.2 Update

Overview
This enables the Data Controller to maintain Business Function Accesses by assigning authorities to Data Subjects and other requirements at a group or organisation level.

Primary User
Data Controller

Starting Point
When the user elects to update Business Function Accesses.

Ending Point
When the information has been validated and processed by the system, and the user is informed of the success or failure of the operation.

Measurable Result
The Business Function Accesses records are updated.

Flow of Events
Check that the SessionID supplied is valid and current, and establish authorisation to perform this function (Check Authority).

Changes will be confirmed with the user before being applied. All data should be validated both prior to

confirmation and prior to update, and the user notified of any errors and given the opportunity to correct them.

Before applying changes to the database, it should be checked to ensure that another user has not updated the same data in the period between this user first viewing it and subsequently making a change. Where this is the case the update should be refused, and the user should be returned to the update screen showing the latest information from the database.

Alternative flow of events
Data entered fails validation, in which case the user is informed of the issue(s) and is invited to re-try the update after correction.

Or, the user is denied access due to lack of authority, or is referred back to theLog-on page because their SessionID is invalid or has expired.

3.7 USERNAME/PASSWORD MAINTENANCE
(See 2.4, USERNAME/PASSWORD)

3.7.1 View

Overview
This enables the user to view usernames, passwords, Data Subject names, and Data Subject ID numbers.

Primary User
Data Controller

Starting Point
When the user requests a list of usernames, passwords, Data Subject names, Data Subject ID numbers.

Ending Point
When the information has been presented to the user.

Measurable Result
The username/password information is presented to the user.

Flow of events
Check that the SessionID supplied is valid and current, and establish authorisation to perform this function (Check Authority).

Build and display the list of usernames, passwords, Data Subject names, Data Subject ID numbers based upon data held on the system (see 2.4, USERNAME/PASSWORD).

The function will break the list of details into manageable chunks, and provide controls to allow the user to page backwards and forwards between them, or to jump to any other chunk.

Alternative flow of events
The user is denied access due to lack of authority, or is referred back to theLog-on page because their SessionID is invalid or has expired.

3.7.2 Update

Overview
This enables the user to update usernames, passwords, Data Subject names, Data Subject ID numbers, and the dates on which a given Data Subject consented to the Specified Processing. It also includes functionality to allow a Data Subject Force Password Change.

Primary User
Data Controller

Starting Point
When the user submits amended details relating to a list of usernames, passwords, and Data Subject names, Data Subject ID numbers, and whether the Data Subject Force Password Change is required.

Ending Point
When the information has been validated and processed by the system, and the user is informed of the success or failure of the operation.

Measurable Result
The details are updated as requested.

If the user requires a new password, for whatever reason, confirmation of their identity is undertaken, and then the Data Controller can set a new password for the Data Subject.

Flow of events
Check that the SessionID supplied is valid and current, and establish authorisation to perform this function (Check Authority).

Validate the data entered and submit the changes to the database.

Alternative flow of events
Data entered fails validation, in which case the user is informed of the issue(s) and is invited to re-try the update after correction.

Or, the user is denied access due to lack of authority, or is referred back to theLog-on page because their SessionID is invalid or has expired.

3.7.3 Delete

Overview
This enables the user to delete usernames, passwords, Data Subject names, and Data Subject ID numbers.

Primary User
Data Controller

Starting Point
When the user chooses to delete details relating to a list of usernames, passwords, and Data Subject names, Data Subject ID numbers.

Ending Point
When the deletions have been applied to the database or have been cancelled due to failure.

Measurable Result
The requested deletions are applied.

Flow of events
Check that the SessionID supplied is valid and current, and establish authorisation to perform this function (Check Authority).

Delete the selected data from the database.

Alternative flow of events
The deletion fails, in which case the user is informed of the issue(s).

Or the user is denied access due to lack of authority, or is referred back to theLog-on page because their SessionID is invalid or has expired.

3.8 MAINTAIN NEW SPECIFIED PROCESSING

Overview
Allows a Data Controller to create a new version of the Specified Processing text and to provide a date from which it is effective.

Primary User
Data Controller

Starting Point
When the Data Controller requests the New Specified Processing option.

Ending Point
When the New Specified Processing details have been updated or the action has been cancelled due to failure.

Measurable Result
The New Specified Processing details are added to the database and the DataSubjectSpecifiedProcessingAgreed flag, Date field and Consent fields for all Personal Data Items are set to N.

Flow of events
Check that the SessionID supplied is valid and current, and establish authorisation to perform this function (Check Authority).

The Data Controller enters the New Specified Processing text. The submission of this information updates the NEW SPECIFIED PROCESSING table.

The DataSubjectSpecifiedProcessingAgreed and AgreedDate fields are set to N and NULL respectively. Also, all the Personal Data Item Consent flags are set to N, requiring the Data Subject's fresh consent at next Log-on.

Alternative flow of events
Data entered fails validation, in which case the user is informed of the issue(s) and is invited to re-try the update after correction.

Or, the user is denied access due to lack of authority, or is referred back to theLog-on page because their SessionID is invalid or has expired.

3.9 MAINTAIN DATA ITEM

3.9.1 View

Overview
This enables the Data Controller to view how Data Items relate to Default Processing Groups. A Data Item's Default Processing Group to defines the way in which a Personal Data Item can be processed before consent is received from the Data Subject. The Function Notification record to which the Data Item is associated is also displayed.

Primary User
Data Controller

Starting Point
When the user elects to view Data Items.

Ending Point
When the information has been presented to the user.

Measurable Result
The Data Item information is presented to the user.

Flow of events
Check that the SessionID supplied is valid and current, and establish authorisation to perform this function (Check Authority).
The Data Item Description, the Default Processing Group to which it belongs and the Functional Notification title to which it is associated are presented to the user.

Alternative flow of events
SessionID is invalid or has expired.

3.9.2 Add

Overview
This enables the Data controller to add a Data Item and to define its Default Processing Group and Function Notification settings.

Primary User
Data Controller

Starting Point
When the user enters new information for a Data Item and its associated Default Processing Group and Function Notification.

Ending Point
When the information has been validated and processed by the system, and the user is informed of the success or failure of the operation.

Measurable Result
A Data Item and its association to both Default Processing Group and Function Notification are added to the database.

Flow of events
Check that the SessionID supplied is valid and current, and establish authorisation to perform this function (Check Authority).

The Data Item description is entered and must not exceed twenty characters. The Default Processing

Group for this item must be selected along with the Function Notification title before being submitted.

On validating correctly, the data will be written to the DATA ITEM table.

Alternative flow of events
Data entered fails validation, in which case the user is informed of the issue(s) and is invited to re-try the update after correction.

Or, the user is denied access due to lack of authority, or is referred back to theLog-on page because their SessionID is invalid or has expired.

3.9.3 Update

Overview
This enables the Data Controller to update the Data Item's association to a Default Processing Group and to a Function Notification record.

Primary User
Data Controller

Starting Point
When the user elects to amend Data Item information.

Ending Point
When the information has been validated and processed by the system, and the user is informed of the success or failure of the operation.

Measurable Result
Data Item records are updated.

Flow of events
Check that the SessionID supplied is valid and current, and establish authorisation to perform this function (Check Authority).

Changes will be confirmed with the user before being applied. All data should be validated both prior to confirmation and prior to update, and the user notified of any errors and given the opportunity to correct them.

Before applying changes to the database, it should be checked to ensure that another user has not updated the same data in the period between this user first viewing it and subsequently making a change. Where this is the case the update should be refused, and the user should be returned to the update screen showing the latest information from the database.

Alternative flow of events
Data entered fails validation, in which case the user is informed of the issue(s) and is invited to re-try the update after correction.

Or, the user is denied access due to lack of authority, or is referred back to theLog-on page because their SessionID is invalid or has expired.

3.9.4 Delete

Overview
This enables the user to delete Data Item records.

Primary User
Data Controller

Starting Point
When the user chooses to delete Data Items.

Ending Point
When the deletions have been applied to the database or have been cancelled due to failure.

Measurable Result
The requested deletions are applied

Flow of events
Check that the SessionID supplied is valid and current, and establish authorisation to perform this function (Check Authority).

Delete the selected Data Item from the database, providing that it is not currently in use by a Personal Data Item record.

Alternative flow of events
The deletion fails, in which case the user is informed of the issue(s).

Or the user is denied access due to lack of authority, or is referred back to theLog-on page because their SessionID is invalid or has expired.

3.10 MAINTAIN DEFAULT PROCESSING GROUP

3.10.1 View

Overview
This enables the Data Controller to view the Default Processing Groups and the Default Processing associated with them.

Primary User
Data Controller

Starting Point
When the user elects to view Default Processing and Groups.

Ending Point
When the information has been presented to the user.

Measurable Result
The Default Processing and Groups information is presented to the user.

Flow of events
Check that the SessionID supplied is valid and current, and establish authorisation to perform this function (Check Authority).

The Default Processing and Groups information is presented to the user.

Alternative flow of events
The user is denied access due to lack of authority, or is referred back to theLog-on page because their SessionID is invalid or has expired.

3.10.2 Add

Overview
This enables the Data controller to add a Default Processing Group and to define its Default Processing.

Primary User
Data Controller

Starting Point
When the user enters new information for Default Processing Group and its associated Processing.

Ending Point
When the information has been validated and processed by the system, and the user is informed of the success or failure of the operation.

Measurable Result
A Default Processing Group and its Processing information are added to the database.

Flow of events
Check that the SessionID supplied is valid and current, and establish authorisation to perform this function (Check Authority).

The Default Processing Group and its Default Processing for this item must be entered before being submitted. On validating correctly, the data will be written to the DEFAULT PROCESSING GROUP table.

Alternative flow of events
Data entered fails validation, in which case the user is informed of the issue(s) and is invited to re-try the update after correction.

Or, the user is denied access due to lack of authority, or is referred back to theLog-on page because their SessionID is invalid or has expired.

3.10.3 Update

Overview
This enables the Data Controller to update the Default Processing Group information.

Primary User
Data Controller

Starting Point
When the user elects to amend the current Default Processing Group information.

Ending Point
When the information has been validated and processed by the system, and the user is informed of the success or failure of the operation.

Measurable Result
Default Processing Group records are updated.

Flow of events
Check that the SessionID supplied is valid and current, and establish authorisation to perform this function (Check Authority).

Changes will be confirmed with the user before being applied. All data should be validated both prior to confirmation and prior to update, and the user notified of any errors and given the opportunity to correct them.

Before applying changes to the database, it should be checked to ensure that another user has not updated the same data in the period between this user first viewing it and subsequently making a change. Where this is the case the update should be refused, and the user should be returned to the update screen showing the latest information from the database.

Alternative flow of events
Data entered fails validation, in which case the user is informed of the issue(s) and is invited to re-try the update after correction.

Or, the user is denied access due to lack of authority, or is referred back to theLog-on page because their SessionID is invalid or has expired.

3.10.4 Delete

Overview
This enables the user to delete Default Processing Group records.

Primary User
Data Controller

Starting Point
When the user chooses to delete details of a Default Processing Group.

Ending Point
When the deletions have been applied to the database or have been cancelled due to failure.

Measurable Result
The requested deletions are applied.

Flow of events
Check that the SessionID supplied is valid and current, and establish authorisation to perform this function (Check Authority).

Delete the selected Default Processing Group record from the database, providing that no Default Processing Group is in use by a Data Item record.

Alternative flow of events
The deletion fails, in which case the user is informed of the issue(s).

Or the user is denied access due to lack of authority, or is referred back to theLog-on page because their SessionID is invalid or has expired.

3.11 MASS DATA ENTRY

Overview
This function allows data relating to Data Subjects to be loaded into the database in batches. This is an offline function carried out by the system's Database Administrator (DBA), and as such does not require the same authentication checks as the online web-facing functions.

Primary User
Database Administrator

Starting Point
On receipt of the Data Subjects' Personal Data Items for mass data entry, the Database Administrator elects to import the data.

Ending Point
When tThe data has been imported into the database and/or an exception report of failures has been produced.

Measurable Result
New Data Subjects' Personal Data Items are available on the database, or all have been rejected due to validation failures.

Flow of events

Validate the data received for import (see 2, Business Design, for details). On successful validation, insert data into the database using the rules specified (see 2, Business Design, for details).

Duplicate names must be signalled, so that the Data Controller can validate whether they are duplicated or not, before the allocation of the Data Subject ID number.

Alternative flow of events
Validation fails and an exception report is produced.

3.12 LOGIN

(See 2, Business Design, for details).

Overview

Authenticate username and password details, and if valid allow users to access the system beyond the Log-on page. If the user is a Data Subject, ask them to change their password if necessary, and ask them to consent to the Specified Processing terms if they have not already done so.

Primary User

Data Subject
Data Controller

Starting Point

When a user navigates to the system's Log-on portal.

Ending Point

When the user has been granted or denied access to the system beyond the Log-on page.

Measurable Result

The user will be granted or denied access to the system beyond the Log-on page.

Flow of events

Use the supplied username to determine whether the user is a Data Controller or a Data Subject. If the user is a Data Controller skip the next paragraph.

If the User is a Data Subject, check whether they have consented to the latest Specified Processing terms; indicated when the **DataSubjectSpecifiedProcessingAgreed** field is set to Y. If not, invite their consent. If consent is given, update the **DataSubjectSpecifiedProcessingAgreed** field to Y and continue processing, otherwise send an email to the Data Controller, and refuse the Data Subject further access to the system.

Check the **UserForcePasswordChange** field. If it is Y, then ask the user to supply an new password, then continue processing.

Check the supplied password against the **UserPassword** field. If they do not agree, notify the user and refuse further access to the system.

If the username and password are valid generate a unique SessionID and update the **UserSessionID** field with the new value. Set the the **UserLastAccess** field to hold the current timestamp. Return the SessionID

Alternative flow of events

The supplied username does not exist in the USER table. The user is notified and refused further access to the system.

3.13 CHECK AUTHORITY

Overview
ID Check that the SessionID is valid and current, and if so, determine the user's authority to perform access the requested Business Function.

Primary User
Data Subject
Data Controller

Starting Point
When a user attempts to use a Business Function.

Ending Point
When the SessionID has been checked, and the authority to perform the requested Business Function is established.

Measurable Result
The User's UserID is returned, or else a value of –1 if the SessionID is invalid or has expired. If the SessionID is valid, then the user's authority to perform the requested Business Function is also returned.

Flow of events
Use the SessionID to query the USER table.

If no matching records are found the SessionID is invalid.

If a row is found, check the UserLastRequest time to determine whether the SessionID has expired.

If the SessionID is invalid, or has expired, return as UserID of –1.

If the SessionID is both valid and current, check the BUSINESS FUNCTION ACCESS table to determine whether the user has authority to perform the requested Business Function. Return the user's UserID and whether the user has access to the requested Business Function or not.

Alternative flow of events
None.

3.14 CHECK IF DATA CONTROLLER NOTIFICATION REQUIRED

Overview
This function determines whether the Business Function performed requires the Data Controller to be notified via e-mail.

Primary User
Data Subject

Starting Point
When a Data Subject performs a Business Function which affects the database.

Ending Point
When either the Data Controller has been notified that a Data Subject has performed a Business Function, or it is determined that no notification is required.

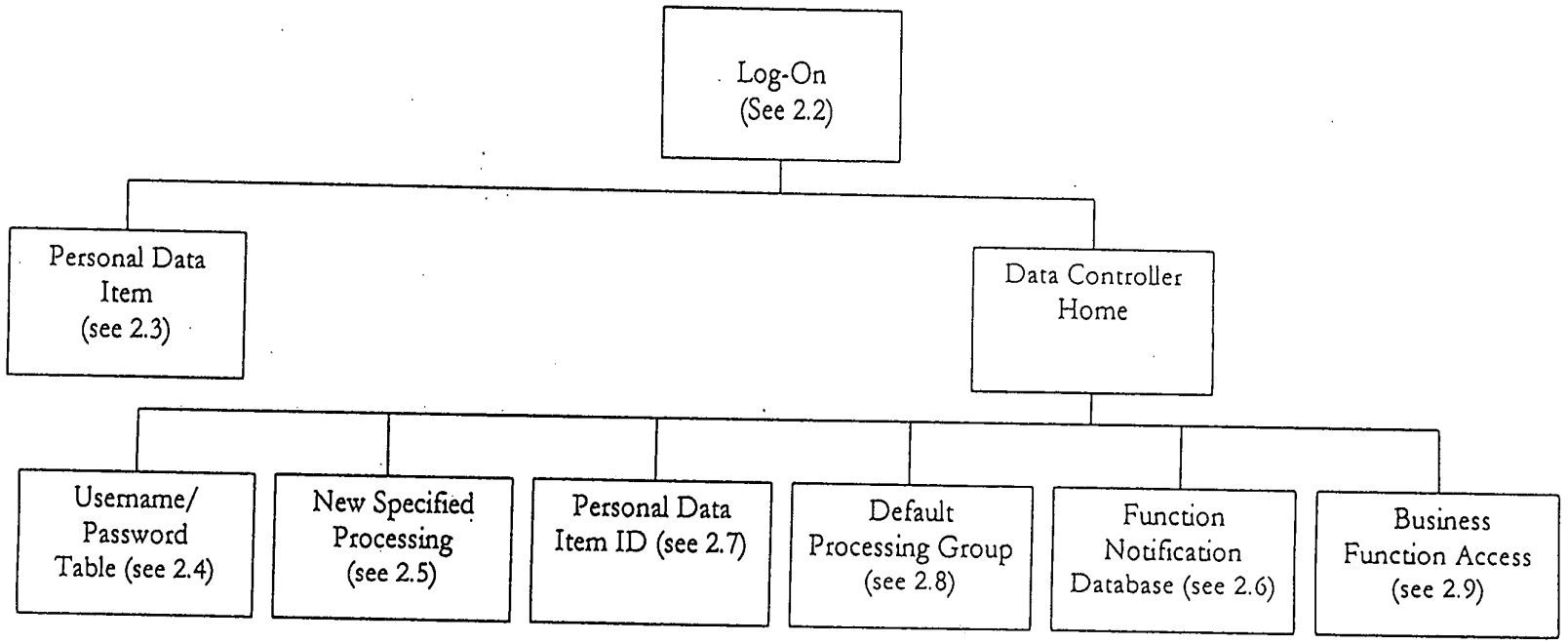
Measurable Result
Either the Data Controller is notified that a Data Subject has performed a Business Function, or it is determined that no notification is required.

Flow of events
Check the FUNCTION NOTIFICATION table to determine whether the Data Controller needs to be notified of this Business Function.

If the Data Controller should be notified, generate and send an e-mail detailing the Business Function performed by the Data Subject.

Alternative flow of events
None.

3.15 SITE DIAGRAM



Date Created: 15/07/00
Date Printed: 15/01/01
Created by: Benjamin Van Every

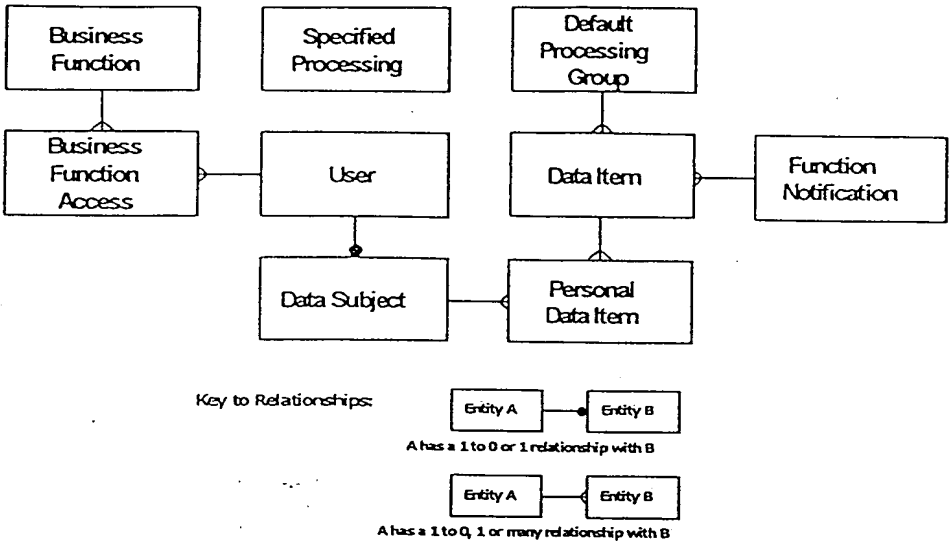
4. DATA MODEL

4.1 Table Classification

All tables are classified into one of two main types.

- Data Subject Table: this carries information about the individual Data Subject
- Maintenance Table: This is a table used to control access to the system or ensure correctness of information entered.

4.2 Logical Entity Relationship Diagram



4.3 Logical Data Definitions

The logical database entity definitions contain the following headings:

- Item Description (with a * if it is the primary key or part of the primary key)
- Optional/ mandatory indicator
- Relationship – if this item relates to an entry on another entity
- Notes

BUSINESS FUNCTION	Defines each business function within the system		
Item description	Optional/ Mandatory	Foreign Key relating to:	Notes
*BusinessFunctionCode	M		
BusinessFunctionTitle	M		

BUSINESS FUNCTION ACCESS	Defines a user's access to the business functions		
Item description	Optional/ Mandatory	Foreign Key relating to:	Notes
*UserID	M	User	User number used as the internal key to the system – system generated
*BusinessFunctionCode	M	Business Function	
BusinessFunctionAccess	M		Enquire or Update

DATA ITEM	Defines a data item		
Item description	Optional/ Mandatory	Foreign Key relating to:	Notes
* DataItemID	M		Data Item number used as the internal key to the system – system generated
DataItemName	M		
FunctionalNotificationID	M	FunctionalNotification	
DefaultProcessingGroupID	M	DefaultProcessingGroup	

DATA SUBJECT	Holds the basic information for each Data Subject on the system		
Item description	Optional/ Mandatory	Foreign Key relating to:	Notes
* DataSubjectID	M		Data Subject number used as the internal key to the system – system generated
DataSubjectName	M		
UserID	M	User (User ID)	
DataSubjectSpecifiedProcessingAgreed	M		Y if agreed to specified processing; N if not; default is N
DataSubjectSpecifiedProcessingAgreedDate	M		Date that the Data Subject agreed to the Specified Processing terms

DEFAULT PROCESSING GROUP	Allows default consents to be set up for a group of data items		
Item description	Optional/ Mandatory	Foreign Key relating to:	Notes
* DefaultProcessingGroupID	M		
DefaultProcessingGroupTitle	M		
DefaultProcessingGroupConsentDefault	M		Y or N; default is N

FUNCTIONAL NOTIFICATION	Controls whether e-mails are sent to the Data Controller when Personal Data Item is changed by the Data Subject, and to which address they are sent		
Item description	Optional/ Mandatory	Foreign Key relating to:	Notes
* FunctionalNotificationID	M		
FunctionalNotificationTitle	M		
FunctionalNotificationRequired	M		Y if changes are to be notified; N if not; default is Y
UserID	O	User	User to whom e-mail will be addressed. Mandatory if required is Y and user must be a Data Controller

PERSONAL DATA ITEM	Contains Personal Data Item of Data Subject		
Item description	Optional/ Mandatory	Foreign Key relating to:	Notes
* DataSubjectID	M	Data Subject	
* DataItemID	M	Date Item	
PersonalDataItem	M		
DateLastCorrect	M		Full date and time stamp
LastChangedBy	M	User (User ID)	
LastChangedOn	O		Date field – time held as zeros
Consent	O		Y or N, not set use display default

SPECIFIED PROCESSING	Defines the specified processing text to be displayed. Contains only one row and is only accessed by the Data Controller		
Item description	Optional/ Mandatory	Foreign Key relating to:	Notes
* SpecifiedProcessingID	M		The value 1
SpecifiedProcessingText	M		
LastChangedBy	M	User (User ID)	The user will be a data controller
LastChangedOn	O		Date field – time held as zeros

USER	Contains user-related details		
Item description	**Optional/ Mandatory**	**Foreign Key relating to:**	**Notes**
*** UserID**	M		System generated
UserName	M		Unique name that user uses to sign onto system
UserPassword	M		Held encrypted on the database
UserSessionID	O		Unique SessionID generated by the system at each successful log-on
UserLast Access	O		A timestamp entry updated each time this user access a Business Function
UserDataController	O		Y if user is Data Controller
UserDataSubject	O		Y if user is Data Subject
UserDataControllerE-mail	O		E-mail address of Data Controller
UserForcePasswordChange	M		Y requires password change by user, N does not require change of password